**[Начало записи][00:00:00]**

Своими словами – я рекомендую вам почитать книгу Максима Ильяхова «Пиши, сокращай». Она позволяет научиться писать информативные тексты без воды, без номенклатурщины и бюрократизма. То есть понятным языком. Очень классная книга, частично сделана в виде комикса. Далее. Как определить, что у нас частично выполнена, полностью выполнена, или не выполняется, или не требует выполнения? Например, что у нас понимается под соблюдением правомерности, справедливости и открытости обработки персональных данных? Первое – правомерность. То, что обработка является законной. Что значит – законной? Есть законные основания на обработку персональных данных. у нас в шестой статье, артикул шесть, указаны все правомерные основания на обработку персональных данных. поэтому мы смотрим, все ли виды обработки персональных данных у нас имеют законные основания.

Далее у нас идет справедливость. Справедливость – это значит, что мы не дурим физлицо при сборе его персональных данных, что справедливо берем согласие на законном основании, то есть своими возможностями, как оператор персональных данных, или как контролер мы не злоупотребляем. То есть мы не стараемся впихнуть больше данных, мы не стараемся его принудить поставить согласие, галочку, дать свои данные. Это справедливость.

Открытость – это значит, что у нас все отражено публично, то есть информация о том, как обрабатывать персональные данные, (нрзб.) (00:02:43), может на отдельной страничке – неважно как. Человек видит, какие данные о нем обрабатываются, на каком основании, куда передаются, сколько, кем, какими лицами обрабатываются, как свои права исполнить, позиция компании о том, как она эти данные обрабатывает, специальные данные как обрабатывает, по детям (00:03:03) данные обрабатывает и так далее. То есть в этом случае это подразумевается.

Стоит понять, что из принципов в статье пять исходят все остальные положения (нрзб.) (00:03:17), то есть принципы основополагающие, из них уже все остальные требования, как их соблюдать. Поэтому, чтобы понять, где здесь справедливость, открытость и правомерность… Смотрите – правомерность по каждому процессу, то есть в цели обработки персональных данных, у нас есть законные основания согласно статьи шестой. По всем этим целям при сборе персональных данных, данные собираются справедливо. То есть мы не принуждаем человека поставить галочку обязательно. То есть, если необходимо зарегистрироваться на сервисе, и у настам имеется галочка на ссылке, а человеку не дают зарегистрироваться без поставленной галочки, это значит, что это несправедливая обработка. Каждую цель, цель равно процесс, раскладываем по этому пункту, чтобы понять – справедлива или не справедлива. И открытость то же самое. Смотрим и понимаем, все ли цели обработки данных, все ли обрабатываемые данные, третьи лица, которым передаем и сроки хранения отображены публично в политике, либо в (нрзб.) (00:04:30), либо где-то еще.

Исходя из этого, мы пишем свое заключение. То есть, например, по всем процессам заказчика, кроме… соблюдается справедливость, открытость и правомерность. По такому-то процессу отсутствует правомерность обработки на текущий момент. Важно – мы пишем документ на текущий момент. Мы не приукрашиваем. Если мы приукрашиваем, то мы даем человеку ложную картину. Компания же нас нанимает ни для того, чтобы мы закрыли на все глаза и сказали (нрзб.) (00:05:04).

**[00:05:04]**

Нет. Текущая ситуация должна быть, потом у нас план мероприятий, исходя из написанных рекомендаций. То есть не выполняется – это, если вообще ничего нет по всем процессам. Ни справедливости, ни открытости, ни правомерности по всем целям обработки и процессам. Частично выполняется – это, если хотя бы одна цель обработки персональных данных соответствует этому принципу. Все.

Дальше. Рекомендации по правомерности. Найти законные способы правоприменимости, справедливости, открытости. По правоприменимости еще кое-что хотел сказать. Например, по работникам в Европе не принято брать согласие. В России это частая практика. Там нет. Почему? Есть принуждение, то есть право работодателя, его влияние на физлицо высокое. Если человек не подпишет согласие при трудоустройстве, его не возьмут на работу. Это нельзя (нрзб.) (00:06:31). Если, например, компания собирает персональные данные с работников, когда они трудоустраиваются, и не берет с них согласие, это неправомерно, точнее несправедливо, надо сменить правомерность обработки. То есть несогласие, какие-то законные интересы контролера. Также пишем в рекомендациях по каждой цели обработки данных – как привести в соответствие. То есть правомерность. Если нет правомерности, пишем для каждого процесса, какое правовое основание для обработки мы должны сделать, чтобы все было правомерно. То же самое со справедливостью. По тому процессу, по той цели, где это не исполняется, мы должны дать рекомендацию. И по открытости то же самое. Если чего-то в его политике не хватает или в публичном документе, мы должны написать, что ему там исправить или чем дополнить. Мы не указываем в рекомендациях целую инструкцию огромную. Указать правомерное основание для такой-то цели, или переформулировать цель – вот так, но прям пошагово что ставить, куда ставить, мы не пишем.

По рекомендациям примерно понятно. Пишем их списком. Дальше. Соблюдения сроков хранения персональных данных. Это значит, что для каждой цели обработки персональных данных заказчик, клиент выставил некие сроки хранения. Сроки хранения, сроки обработки. То есть в течение какого времени данные в этих целях будут обрабатываться. Например, у нас есть договор с клиентом, в течение действия этого договора и потом еще три года для защиты интересов в суде контролера, а-ля – срок исковой давности в России. Они должны быть где-то регламентированы в документе. И то, что эти сроки исполняются.

**Как проверим – исполняется или нет?**

На словах только. Иногда мы смотрим реально в системах заказчика, действительно данные удаляются или нет. Скажу честно – чаще всего данные не уничтожаются в большинстве своем. Но это не надо брать за панацею, надо проверять – скриншоты брать, при заказчике на аудите смотреть и запрашивать эту информацию. Также описываем, в каких процессах это исполняется, в каких процессах это не исполняется и почему. И рекомендации то же самое, что нужно сделать. Обычно – это выставить справедливые сроки.

**[00:10:00]**

Вы спрашиваете у заказчика во время интервью, аудита – на самом деле в течение какого времени вам потребуются эти данные? И прописываем там потом – через какой срок уничтожать по факту. Заказчик говорит – мне нужно на все время. А зачем вам на все время? Говорит – ну, чтоб было. Так не работает. Не выполнено ставится, если вообще сроки персональных данных не выстроены и не регламентированы, хранятся бесконечно и не соблюдаются. Частично выполнено – если есть хотя бы по одному процессу сроки хранения, по одной цели. Они где-то описаны и реально исполняются. Это будет частично выполнено. И полностью выполнено – когда мы ставим?

**Если ко всем (нрзб.) (00:11:05) и соблюдаются.**

Да. Все. Компания Yclients. Там, если вы записываетесь на маникюр, в барбершоп или в парикмахерскую онлайн, это скорее всего их сервис стоит на сайтах. Знаете, онлайн-запись есть? Это они самые топовые в России, и мы им помогаем с пиаром.

Первый пункт мы прошли, давайте 1.2, сбор и обработка персональных данных в конкретных ясных и законных целях. Что имеется в виду? Иногда заказчик не понимает, зачем реально данные собирает, типа по маркетингу требуется. А для чего? На потом там или что-то еще. Там точно должны, первое – проверить их цели на конкретность, то есть она не обобщенная, что ее сложно понять или расширить, она прям конкретно для подписки на рассылку и отправки писем. Окей. Они для коммуникации в маркетинге, это очень такое, расплывчатое понятие. Первое – она должна быть законная. Например, для продажи ваших персональных данных – это незаконная цель. И ясная. Ясная – значит, она понятным языком написана. Конкретная – то, что она не обобщенная. Каждую цель мы на это смотрим. У нас могут быть данные без цели. Значит, мы им должны порекомендовать эту цель.

Не выполняется – если у нас все цели или неконкретные, или неясные, или незаконные, если хотя бы одно из трех по всем процессам проходит, все, не исполняется. Если хотя бы одна цель всем трем критериям соответствует, то частично выполняется. В рекомендациях также пишем, как цели переформулировать. То есть, если они неконкретные, то как их сделать конкретными, если цели у нас неясные, сложным языком написаны, то мы их упрощаем и даем, как это упросить. Если незаконные, то говорим, перестать обрабатывать в незаконных целях. Вот и все. Окей.

Далее. Пункт 1.3 – соблюдение условий по обработке достоверных и соответствующих целям обработки персональных данных.

**[00:15:06]**

Что имеется в виду? Как вы думаете? У нас есть цель, чтобы ее исполнить, нам потребуются какие-то данные.

**Чтобы не было избыточно?**

Вот, да. Поэтому стоит все цели посмотреть и понять, являются они избыточными или нет. Честно признаюсь – без опыта это сложно понять. Но самое главное здесь – это критическое мышление. Вам может показаться, что слишком… Чтобы сделать номера ссылки, они (00:16:02) берут телефонный номер. Вопрос – зачем вам телефонный номер? Или если они берут какие-то массивные данные. Еще раз – зачем вам для таких целей такой массив данных? По каждой цели проходимся, исходя из логики, здравого смысла и критического мышления, мы определяем уже. Если хотя бы в одной цели есть избыточные данные, то это выполняется частично. Если по всем процессам у нас много данных, они избыточные – то не выполняется. Если по всем все классно – выполняется полностью. Избыточными, например, у нас являются все сканы, копии просто так – паспортов, любых документов. Берут на всякий случай. По рекомендациям понимаете, что делать, как писать?

**Писать предложить исключить избыточные данные.**

В каждом процессе, где они избыточны, это важно. То есть не просто пишем – исключите все процессы по избыточным данным – нет. конкретный процесс – какие данные. Опять же, так как мы их уже выписали в четвертой колонке те процессы, и какие данные и почему являются избыточными, то просто копи паст делаем. Одной из рекомендаций может быть – найти законные основания для обработки этих персональных данных. То есть другую цель сделаем для заказчика и законные основания, чтобы все-таки пойти на встречу клиенту, потому что мы не должны приходить и говорить – все неправильно, все удаляйте. Нет, так не работает. Мы должны дать несколько рекомендаций, чтобы они имели выбор.

1.4 Соблюдение точности обрабатываемых персональных данных. Что это значит? Что контролер направляет меры на то, чтобы – первое: человек мог сам исправить свои данные, и второе: вы должны дать ему такую возможность по его запросу. Не допускается обработка неточных или устаревших персональных данных. У нас это не исполняется, если у человека нет возможности и права исправить свои данные, то есть не реализован процесс по реализации физлицом права на уточнение своих данных, точности изменения. И у компании нет уведомления о том, что коллеги, пожалуйста, подтвердите свои (нрзб.) (00:18:52), что у вас все точно так же. Если у нас это где-то частично реализовано в каком-то процессе. И полностью, если у него есть: первое – доступ физлиц к своим данным по той или иной цели обработки данных для изменения или уточнения, второе – у компании реализован процесс по правам физлиц по доступу к данным, их уточнению и изменению, третье – компания отправляет запрос, как-то коммуницирует с физлицом и говорит – парень, ты давай, данные уточни, обнови, если они изменились. Раз в полгода – письмом, звонком и так далее. По рекомендациям понятно, что здесь? Окей.

Про сроки хранения мы обсудили.

1.6 Соблюдение целостности и конфиденциальности персональных данных при их обработке. Это значит, что организация принимает меры, направленные на то, чтобы сохранялись такие характеристики безопасности, как целостность и конфиденциальность.

**[00:20:11]**

Вы уже проходили, да? конфиденциальность, целостность и доступность. Здесь только две. Меры должны быть. Конфиденциальность – это, чтобы они не утекли к третьим лицам, которые не имеют доступа, а целостность?

**Чтобы не были повреждены или изменены.**

Вот, да. Для этого нам требуется backup как минимум. Также смотрим по каждому процессу, где данные хранятся. Физлица, которые имеют доступ, четко определены, третьи лица, кому данные передаются, установлены все, и они все отображены где-то. Все серверы, где хранятся, на них обеспечивается целостность, то есть backup и конфиденциальные средства защиты от НСД (00:21:13), антивирусов, (нрзб.) (00:21:16) и так далее. Если у компании ничего нет почти, то не выполняется. Если хотя бы что-то есть, антивирус, то выполняется, но частично.

**У меня вопрос: если такая информация не указана ни в одной из политики, например? Может у них есть, но (нрзб.) (00:21:37).**

Да. Как я говорил, в ваших политиках часть информации неизвестна. Вы можете уточнить у компании, написать им запрос. Но вообще, компания обычно сообщает, какие меры они принимают. У компании, помимо (нрзб.) (00:21:54) часто, особенно у крупных, имеются страницы, типа jpar ready (00:21:58). Там они описывают, как данные защищаются, какие они (нрзб.) (00:22:03) и так далее. В рекомендации вы должны порекомендовать провести GPA (00:22:10), и на этом основании уже внедрить необходимые меры защиты, контроля, так называется, для обеспечения целостности и конфиденциальности персональных данных.

Дальше. Подтверждение соблюдения принципов обработки персональных данных. Здесь все очень просто. Вы должны дать хотя бы какую-то бумажку проверяющему о том, что у нас эти принципы соблюдаются. То есть любые подтверждения. Что это может быть, как вы думаете?

**(нрзб.) (00:22:56), например.**

Окей, что еще?

**Можно на сайте оставить где-нибудь.**

Окей, что еще? Мы должны в случае чего (нрзб.) (00:23:12) показать средства защиты. Можно этот документ показать – вот видите, мы соблюдаем. У нас были несоответствия, мы их исправили (00:23:22), готовы вам показать. Первое: во внешнем документе мы это прописываем, в (нрзб.) (00:23:30) полисе, и, если у нас имеются внутренние документы в (нрзб.) (00:23:38) полисе или в delta protaction (00:23:39) полисе, мы это тоже отображаем.

Но не выполняется ставится, если у него нигде это не отображено, частично, если что-то краем уха где-то отображается, либо мы слышим это от заказчика, выполняется полностью, если первое: он может как-то подтвердить любыми способами исполнение этих прав, и в (нрзб.) (00:24:12) полисе или других документах у него это имеется. В (нрзб.) (00:24:14) полисе это обязательно. По рекомендациям понятно? Окей.

Дальше. Наличие правомерных условий для обработки персональных данных. Это то, что мы проходили в принципах, помните? То есть мы прям копи паст.

Наличие подтверждения получения согласия на обработку персональных данных. В данном случае компания должна доказать, что согласие действительно было получено. Что это может быть? Сохранение лог-файлов того, что галочка была проставлена, сохранение логов того, что на этот email было отправлено письмо с подтверждением того, что он дал согласие, зарегистрировался.

**[00:25:03]**

СМС своеобразная, что ему отправили СМС с ключом, он его ввел и все. То есть подтверждения должны быть. Если cookie – то же самое. Видели, в Европе и Штатах на сайте есть такой баннер – я даю согласие на получение… Тоже надо подтверждать, что человек дал согласие. Есть сервисы специальные, тут на примере – сервис «Cookie бот», он такую плашку дает, там несколько галочек, он сохраняет ip-адрес человека, маску некую, слепок его данных из cookie, чтобы потом доказать, что действительно было получено согласие. Не выполняется ставится, если вообще нигде не сохраняется данных, чтобы подтвердить, что согласие было получено, частично – значит, где-то оно имеется, полностью – если оно повсюду подтверждается. По рекомендациям примерно понятно? То есть какие у нас есть способы? Еще раз. Сохранение лог-файлов, того, что галочка проставлена, нажал кнопку. Второе – использование внешний сервисов типа «Cookie бот» и других, которые сами сохраняют все необходимое, чтобы потом подтвердить, дает нам информацию, что мы это подтвердили. Подтверждение по СМС и подтверждение по email.

Далее. Исполнение условия по получению письменного согласия на обработку персональных данных. Честно, я на практике ни разу не сталкивался с этим, давайте посмотрим на документ закона, чтобы я это вспомнил и освежил память свою. Это у нас статья восьмая. Если в письменной форме получаем, то это должно быть явно, на бланке, на договоре отдельный блок, выделено отдельно ото всех, в одной цели. Чтобы прям четко человек увидел, что это отдельно согласие, там должно быть четко и понятно информировано, какие данные о нем, в каких целях, кто обрабатывает, какие права у него, сколько хранит, кому передает свои контактные данные. То есть как по нашему закону, можно брать за основу и использовать.

Далее. Если человек дает письменное согласие, то берем форму, смотрим. Первое: написано ли ясным языком – это лавное в (нрзб.) (00:29:03). Как определить понятный язык? Если вы хотя бы над одном предложением задумались, тяжело читать. Или если есть термины, которые вам непонятны.

Далее идет информация, которая должна быть в согласии. Данные контролера, его DPO (00:29:29) или представителя, полный адрес с индексом, телефон, email, можно иные способы коммуникации – WhatsApp, Viber, Facebook и так далее.

Далее. Состав данных, которые обрабатываются. Для какой одной цели они обрабатываются?

**[00:30:00]**

Какие законы основные для (нрзб.) (00:30:04) этих данных, пишем просто согласие. То есть данное согласие – это законная цель. Срок хранения или сроки хранения. То есть мы пишем – данные согласия даются на обработку данных, то есть вот так, но потом уже, когда цель прекратит действовать, ваши данные будут хранится вот в такой цели еще три года для защиты наших законных интересов. Мы информируем человека о том, что вот этот промежуток времени данное согласие будет работать, а потом там будут уже наши законные цели и основания. И обработка данных для этой цели в эти сроки не требует от нас твоего нового согласия.

Далее. Смотрим, кому данные поручаются и передаются, в какую страну. Далее. Отдельно прописываем, если передача данных в международную компанию, или передача данных в страны, не обеспечивающие адекватной защиты персональных данных. Сейчас есть только две страны. Есть Евросоюз, есть Европейское экономическое общество, как-то так называется, это Швеция, Норвегия, Люксембург и по мелочи. Япония и Швейцария. Все остальные страны не обеспечивают адекватной защиты, и мы об этом должны предупреждать.

Далее. Информация о том, как человек просто может отозвать свое согласие.

**А это все должно быть указано в письменном согласии на обработку?**

Я рекомендую, да. Он должен быть полностью информирован о том, как и что у него происходит с его персональными данными в этой цели. Право на отзыв. Дальше. (нрзб.) (00:32:09) всех прав физлиц по (нрзб.) (00:32:11), которыми он может воспользоваться. Это можно сделать также в виде QR-кода ссылки на сайт, где отдельно по правам все описано. Все.

Далее. Согласие должно быть обрамлено, явно в тексте выделено. Что это не просто галочку поставить, а что человек понимает, что он подписывает. Это прописано в законе. Не выполняется – ни одно из того, что я сказал, не исполняется, частично выполняется – если что-то из этого исполняется, хотя бы одно, выполняется полностью – если все это совпадает, вся эта информация как-то здесь указана. По рекомендациям примерно понятно? Окей. И также все написано понятным языком. Это базовое требование в (нрзб.) (00:33:17), все документы внешние, все, что читает от вас по (нрзб.) (00:33:20) данным человек, должно быть написано понятным языком. Выполнение не требуется, как здесь, если не собирает письменных форм согласий.

Следующий пункт. Исполнение условий по простому отзыву согласия. В данном случае согласие должно быть также просто отозвано, как он с ним согласился, то есть не надо сложные процедуры проходить. Если у него есть личный кабинет, и он до этого согласился, то он должен просто галочку снять. Если такого нет, то в каждом письме, например, по email-рассылке, должны быть ссылка – отписаться, (нрзб.) (00:34:18) на обработку данных. Если мы начали данные обрабатывать (00:34:27), должны дать какие-то иные возможности на отзыв согласия. Это может быть – введи свой email, и ему дают твой аккаунт или что-то такое.

**[00:35:00]**

Окей. Не исполняется это требование, если все согласия, которые у него есть вообще, либо письменные, либо онлайн, сложно исполняются. Например, в Google, был оштрафован на 50 миллионов. Не знаете? Позавчера новость вышла, что французский регулятор оштрафовал его на 50 миллионов евро. За то, что очень хреново давались согласия, нужно было на пять ссылок перейти, и так же сложно они отзывались. Вот вам пример. То есть согласие должно максимально просто отзываться. Если ни одно просто не отзывается по вашему мнению именно, то вы об этом пишите и пишите – не исполняется. Если хотя бы одно просто отзывается, если, например, в личном кабинете у человека есть галочка – отписаться от рассылки, он снимает галочку и все. Это окей. То выполняется частично. Если все хорошо выполняется в плане отзывы, пишем все выполняется. Важно – вы любую свою позицию перед клиентом, перед компанией – не важно, будете ли работать в консалтинговой компании, либо в штате компании (нрзб.) (00:36:37) внутри, должны уметь обосновывать свою позицию. Все, что вы пишите, вы должны уметь обосновать. Есть такая очень классная книга, я вам ее советую, называется «Пирамида Минто». В чем основной смысл? (нрзб.) (00:37:06) простым языком – не исполняется. Почему не исполняется? На уровень ниже падаем. В общем, в общем, в общем. Дальше может по каждому пойти из пунктов. Почему считаешь, что именно это не исполняется? Понимаете, смысл. Важны доказательства. Это на самом деле очень простая практика. Знаете, как определить пять почему? Например, почему ты хочешь заниматься (нрзб.) (00:37:37)?

**Просто интересно.**

Почему тебе это интересно? Пять раз задаешь и человек доходит до сути. Здесь должны на пять уровней вниз опуститься и иметь законное подтверждение. На последнем уровне у вас должен быть железобетонный аргумент. Если нет аргумента, значит надо подумать – ага, значит стоит пересмотреть свою оценку или рекомендацию.

Поехали дальше. Исполнение условий предоставления согласия на обработку персональных данных по доброй воле. Это то, что я говорил. Первое – согласие есть отдельной галочкой, оно никуда не вшито. Что это значит? Это значит, что одна галочка, и человек по одной галочке соглашается сразу с двумя какими-то пунктами. Это плохо. Потому что он одной галочкой, одним своим действием два действия делает. А это принуждение, это несвобода воли. Например, одна галочка – он соглашается на веб-сайте с правилами сайта, то есть оферта, пользовательское соглашение, и одновременно дается согласие – не работает. Или в договоре в бумажном сразу зашито – будем делать рассылки – нельзя. Далее. Не должно право довлеть, как я вначале говорил, контролер не должен пользоваться своим привилегированным положением, чтобы собирать данные, согласие. То есть работодатель говорит – не дашь согласие, не будешь принят на работу. Или без этой галочки здесь мы не сможем ваши данные обрабатывать в данной цели. Нельзя так делать.

**А если это необходимо?**

Что?

**Например, поставить галочку для обработки персональных данных.**

**[00:40:02]**

Чтобы обрабатывать данные? Значит, ищи другие законные основания. Если услуга не может быть оказана без этого согласия, значит что-то неправильно ты в аудите провела. Не должно быть такого, что услуга оказывается только с согласия. Есть же договор на услугу. Надо или договор расширить на это все, или же найти иные законные основания для обработки данных, для человека. Не может быть такого, что без согласия услуга не может быть оказана по договору. Не выполняется ставится, если у нас есть такие случаи, когда не по доброй воле, выполняется частично, если хотя бы один случай согласие дается все-таки по доброй воле, то есть по справедливой основе, помните – пункт про справедливость? Здесь мы просто более детально это описываем. Там – в каких процессах и почему, здесь уже более конкретно, с ссылками и так далее. Выполняется полностью, если все на справедливой основе. Вы поняли, почему нельзя согласие делать обязательным для оказания услуги?

**А если, например, брать медицинские какие-то данные, то без согласия человека на обработку этих данных, это же будет, получается, незаконно?**

У тебя есть первое – законные основания. В моей парадигме один процесс – это одна цель обработки данных. Для каждого процесса ты должна определить законные основания. Если ты (нрзб.) (00:42:14) законные основания, есть ряд сложностей, потому что много требований к нему. (нрзб.) (00:42:20), например, законодательный акт, в каждой стране есть свой закон. И вы должны его анализировать и понимать – окей, это подходит под это, здесь согласие нам не требуется. При анализе правовой оценки, правового обоснования обработки персональных данных, вы должны анализировать не только (нрзб.) (00:42:45), но еще и те страны, где работает заказчик в Европе. Анализировать их локальный (нрзб.) (00:42:56). То есть каждая страна принимает один в один закон (нрзб.) (00:43:00), но у них могут отличаться законные основания для обработки данных. Шире могут быть. поэтому смотрите их. Google translate вам в помощь.

Далее. Выполнение условий обработки чувствительных категорий персональных данных. Кто мне скажет, что у нас относится к чувствительным категориям персональных данных?

**Аналитическая предрасположенность, (нрзб.) (00:43:31), семейное положение, возможно, медицинские какие-то… Группа крови. Религия, ориентация.**

Окей, да. Биометрия, сведения о здоровье, сведения о судимости – это важно. Судимость тоже относится сюда. У нас есть определенные законные основания для обработки этих данных. Первое – согласие. Второе – законодательство той страны, где это требуется. Далее. Для выполнения целей по осуществлению конкретных прав контролера в области занятости, социального обеспечения и социальной защиты. Опять же, смотрим на законодательство той страны. Далее. Обработка осуществляется для защиты жизни человека. Если он физически недееспособен дать свое согласие.

**[00:45:00]**

Его сбил автомобиль, мы ничего не можем сделать, поэтому будем данные обрабатывать сами. Приехали в клинику, определили кровь, возраст и так далее. Дальше. Обработка относится к персональным данным, которые явно являются обнародованными. То есть там есть исследования, он заранее дал согласие на (нрзб.) (00:45:29) в журналах, есть научные журналы, там пишется про это все. Для суда, то есть для подачи заявки в суд, (нрзб.) (00:45:44) дела. Обработка данных необходима для поддержания общественного интереса и прав общества. Например, у нас есть какая-нибудь Эбола, все в срочном порядке сдают кровь и данные обрабатывают. Извините, ваши данные, хотите вы или нет, будут обработаны. Для работника, если требуется для профилактики или медицинского труда по оценке работоспособности, анализы или медицинского, социального ухода, лечения и здравоохранения. Тоже закон. По факту медицинские услуги чаще всего будут иметь законные основания. Дальше. В целях ведения архива, научной деятельности, исторических исследований и так далее. При этом должна обязательно сохраняться тайна.

**У меня вопрос по поводу исторических исследований. Если это касается какой-то конкретной компании, ее сферы деятельности, любая компания может сказать, что ей нужны ваши данные (нрзб.) (00:47:21).**

Нет, ты скажешь – мы решили создать фонд. Есть разные исторические фонды. (нрзб.)(00:47:29) Сталин болел вот этим. Мы писали книгу о том, что было в Чернобыле «Они еще живы», мы брали часть записей из архива, а там были данные этих людей, которые тогда заболели этой лучевой болезнью. Окей. Вопросы? Окей.

Обработка сведений о судимости возможна только под контролем властей той страны или госорганов. Не исполняется это требование полностью, если у нас есть несколько целей с этими данными, и нет законных оснований. Они или не определены, либо определены неверно. Выполняется частично, если по части таких целей у нас имеются законные основания для обработки этих данных. Выполняется полностью, если все классно. Под законным основанием мы должны найти конкретную статью конкретного закона, который (нрзб.) (00:48:47) законодательством обрабатывается. И расписать это дело. Если у нас есть общественный интерес, пишем, в чем именно заключается этот общественный интерес, и почему мы считаем его общественным интересом. Окей. Вопросы по чувствительным персональным данным? Нет, окей.

Пункт 1.14 предоставление информации субъекту данных в установленные сроки. У него есть свои запросы, он может своими правами воспользоваться, нам написать, позвонить и так далее. То есть оставить нам запрос. Срок (нрзб.) (00:49:47) 30 календарных дней, запишите, это очень важно, из-за этого один наш клиент уже пострадал.

**[00:50:00]**

Если запрос сложный, требуется время на реализацию права человека или на ответ, то можем продлить еще на 60 дней. То есть общий срок ответа будет 90 дней с момента… Опять же, до 60 еще сверху. Вы должны заранее точно определять, сколько точно времени вам еще нужно сверх 30 дней. Это должны быть явные основания. Имеется в виду, что мы не просто так увеличили срок, что нам в падлу в 30 дней укладываться. Должны быть веские причины. Время, ресурсы требуются или новогодняя загруженность. В новый год исторически много заказов на доставку из наших магазинов. Мы перегружены, поэтому извините, можем увеличить срок. Увеличение срока еще на 60 дней или на сколько-то сверху, мы должны человека уведомить в первые 30 дней и написать ему причину продления срока. Далее. Информацию о сроках ответа и возможностях продления до 90 дней с момента получения запроса, вы должны прописать в своих документах публично. В согласиях, в (нрзб.) (00:51:44) полисе.

**А здесь имеется в виду предоставление информации в том плане, что, например, пользователь решил узнать, удалена ли о нем какая-то персональная информация, это в таком плане? Предоставление информации субъекту данных – это та информация… Он спросил – уладили ли о нем…?**

Да, любой запрос, касающийся (нрзб.) (00:52:19) прав, да. у него есть права, мы об этом чуть дальше поговорим. Далее. Бывают навязчивые вопросы. Мы заказчику дали ответ, и он пишет такой же запрос. Можно считать, что это не объективный запрос и злоупотребление правом. В этом случае мы должны ему отказать и описать, почему – коллега, мы тебе уже отвечали, это повторение твоего же вопроса недельной давности. Либо сказать – да, мы вам ответим, но это будет стоить столько-то. Это прям в законе прописано. Стоимость должна быть равна стоимости издержек компании на (нрзб.) (00:53:01) запрос. То есть часы человека, сколько мы должны дать ему за это.

Дальше. Пункт 1.15 уведомление человека об обработке его персональных данных. Что это такое? Это (нрзб.) (00:53:36), это документ, в котором прописано то же самое, что в согласии, но только по всем внешним категориям субъектов данных. Что имеется в виду? Посетители сайта, те, кто подписались на рассылки, контрагенты, партнеры, кандидаты на вакантные должности, те, кто пишет формы обратной связи, наши клиенты – всех там описываем. То есть только внешние, по работникам, по контрагентам нашим, с которыми у нас договор, мы не пишем, будет отдельный документ у нас. То есть в (нрзб.) (00:54:18) обычно пишется внешний документ, который будем всем показывать, и (нрзб.) (00:54:22) показываем только работникам, их родственникам и контрагентам, то есть всем тем, кто с нами работает внутри, и мы не хотим палиться (00:54:30) сверху.

По предыдущему пункту не выполняется предоставление (00:54:41) информации, если у нас это не отображено по срокам, и потому что можем игнорировать его запрос, если он неадекватный, или брать деньги в (нрзб.) (00:54:55) полисе или в staff-полисе (00:54:58). Мы должны это указать публично.

**[00:55:00]**

Если мы это не указываем, это не выполняется, и если что-то указано частично, и если в обоих документах или в единственном документе, который имеется, публично это есть, то все окей.

По (нрзб.) (00:55:20) нотис. Если у нас есть работники в Евросоюзе (00:55:24), мы делаем в staff-полисе (00:55:26), то есть еще раз – внешняя политика, внутренняя политика. Понимаете логику, зачем это требуется все?

**Да.**

Окей. Не исполняется, если нет такого документа в принципе, ни внутреннего, ни внешнего. Второе – частично исполняется, если хоть какая-то информация хоть о какой-то цели, что-то из этого большого перечня, или данные указаны, или цель указана хоть одна, то частично исполняется. Или одно право человека указано, или контакт. То есть что-то есть. Полностью исполняется, если у нас есть в (нрзб.) (00:56:12) полисе на работников и на внешний субъектов, и там все указано. Важно еще – это все указано понятным языком. Я поэтому вам рекомендую почитать «Пиши, сокращай». Эта книга, по-моему, у нас здесь лежит, мы заказывали. Я могу вам ее дать почитать.

**В интернете найдем.**

Окей. Просто на бумажной книге удобнее читать и делать пометки. Окей, вопросы? Давайте первый блок пройдем, потом перерыв.

Далее. Пункт 1.16 предоставление информации при получении персональных данных не субъектом данных. То есть, если у нас это имеется, например, мы для скоринга физлиц, которые обратились к нам за кредитом… Знаете, что такое скоринг? Это проверка на платежеспособность. Каждому из нас дается свой разный балл, и есть некий порог. Людям с этим баллом мы даем кредит и в таком объеме, этим нет. Мы должны написать информацию о том, какие данные берутся для скоринга. Это обычно из налоговой, из базы кредитных историй и так далее. То есть мы об этом должны публично заявить, если такое имеется. Или мы ваши данные получаем от таких-то контрагентов изначально. Также об этом надо информацию там отразить. Первое. Не исполняется, если человек не отразил публично, что он в принципе получает эти данные, то есть он публично это не отразил, либо же имеется получение данных от третьих лиц, то есть из внешних источников, но мы это не указали. Частично исполняется, если хотя бы один источник там указан, полностью выполняется, если у нас указаны все источники, если они оттуда собирают данные. Ниже написано, что мы данные не собираем из внешних источников. То есть это налоговые, банки данных, обогащение данных.

**То есть не выполнено будет в том случае, если мы не указали, что будет собрана информация…?**

Если она по факту собирается из внешних источников, то мы должны это указать. Если это не отображено, то не исполняется. Если мы не собираем из внешних источников, но мы это не заявили публично, то тоже будет являться неисполнением.

**[01:00:00]**

О'кей. Поехали дальше.

Выполнение прав субъектов персональных данных на доступ к персональным данным. Первое. По запросу физлиц мы должны отвечать на следующие запросы, а именно: о цели обработки персональных данных, о соответствующих категориях обрабатываемых данных, то есть общедоступные, иные чувствительные данные, обезличенные. О получателях персональных данных третьих лицах, в третьих странах и международных организаций, кому данные передаем. О сроках обработки персональных данных или условиях, когда прекратится обработка персональных данных.

О наличии своих прав требовать от контроллера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки. О праве подачи жалобы в надзорный орган. То есть мы должны показать, что, парень, ты можешь подать на нас жалобу в надзорный орган. Об источнике любой информации, связанной с его персональными данными, и если они получены из третьей стороны, источника внешнего. О применении автоматизированной обработки, и есть она или ее там нет, то указываем, как работает этот алгоритм автоматизированный. О передачи в страны, которые не обеспечивают адекватной защитой прав субъектов персональных данных.

И есть о гарантиях. То есть у нас гарантии передачи такой стороной. Мы об этом потом поговорим. Важно. На доступ к данным мы также должны выгрузить данные о нем и дать ему, какие данные вы обо мне обрабатываете. Вы можете указать вот такие категории данных. То есть, дайте доступ к этим данным, я хочу видеть, какие именно данные вы обрабатываете, и должны выгрузить.

Если все эти пункты публично не отражены, то не отображена непублично, и у нас внутри не регламентирован каким-либо документом, инструкцией, памяткой процесс реализации прав этих физлиц, то не исполняется. Если есть или внутренняя инструкция, или регламент, или памятника, или в privacy policy что-то частично указано о том, какие права могут реализоваться, то пишем «частично». Если все исполняется, – то все полностью. Вопросы? Отлично.

**А на практике часто было такое, когда полностью исполняется этот пункт?**

Да, конечно, естественно. А на моей практике?

**Да.**

Ни одной. Чтобы полностью – ни одной, чтобы частично, – да. Часто есть инструкции, и часто есть хотя бы часть информации в privacy policy. О'кей.

1.18. Выполнение прав субъектов персональных данных на исправление персональных данных. То есть человек имеет право поправить или по запросу изменить свои персональные данные, если они неточные, либо же иметь best practice, то есть лучшая практика, это если есть доступ у него самостоятельно к своим данным, что он может их сам исправить онлайн. Это должно быть также отражено в политике, что такое право у него есть, и как он может им воспользоваться. И в локальном документе, памятке, инструкции.

Не исполняется, если у нас в privacy policy это право, как оно реализуется, не отражено, и нет внутренних документом, которые хоть как-то регламентируют исполнение этого права физлицом.

Если все исполняется, скажем так, про частичное исполнение мы хотя бы что-то где-то указываем, если полностью не выполняется, то дописываем в этих рекомендациях best practice, типа, дайте доступ людям к данным онлайн, если это возможно.

[01:05:17]

**Например, у человека изменилась фамилия, но паспорт ему еще новый не выдали.**

По факту паспорта он должен сообщить.

**То есть, как только ему дадут новый паспорт...**

Да, конечно. Если сменилось имя, в документе, свидетельстве о браке уже написано изменение фамилии, о'кей, можем уже сказать: измените. Если контроллер данный паспорт обрабатывает, вы сообщаете о том, что это требуется тоже изменить.

Дальше идем. Выполнение прав субъектов персональных данных на удаление его персональных данных. То есть человек имеет право на удаление своих персональных данных. То же самое, должно быть отражено лично, и во внутренних документах есть какая-то справка о том, как это исполняется. Частичное исполнение, это если что-то есть, и полное, если все есть. Важно, есть случаи, когда данные могут быть не удалены. Это также публично надо отразить. Это когда данные обрабатываются для осуществления прав и свобод на выражение мнений и распространение информации. То есть человек может, что угодно писать, или СМИ. Если человек это пишет, то есть у него цель не просто всю информацию на другого человека высказать, а то, что такой-то человек у нас работал, вот так-то, так-то, нам это не понравилось. То есть цель была показать практику общую, и не было цели именно эти данные специально показать. Просто они под контекст подходят, понимаете? Если же специально выложены данные о человеке зачем-то, это незаконно. Их надо удалить.

Для соблюдения правовой обязанности, которая установлена Евросоюзом, или для задачи в общественных интересах, или для официальных полномочий, то есть все описано, возложенных на контроллера. Что это может быть. Например, есть общественный интерес на получение достоверной информации, или получение информации из разных источников. Если мы сталкиваемся с человеком на видео в ходе репортажа, или в ходе, не знаю, мы художники, мы людей нарисовали, просто, Париж, Сена, мы рисуем, там какие-то люди, часть нарисовали. Говорят: «Удалите». Нет. Общественный интерес на культурное наследие, sorry.

В силу общественных интересов в сфере социального здравоохранения. То есть мы не должны удалять данные о том, чем человек болел. Есть какие-то опасные социальные заболевания, туберкулез, например. Sorry, но мы не можем это удалить. Также для архивных целей, научных, исторических и статистических целей. Или если компании эти данные требуются для защиты своих интересов в суде. То есть судятся они, либо срок исковой данности у нас еще имеется. Мы это все должно доводить публично, всю информацию, чтобы человек понимал.

Выполнение права на ограничение обработки по персональным данным. Пример. Человек имеет право заблокировать свои персональные данные, например, если у него есть суд, и ему эти данные требуются, то есть он боится того, что данные контроллер удалит, а ему они требуются для доказательства своей позиции в суде, либо в спорах с этим контроллером. Он прямо так и говорит: «Заблокируйте мои данные». Рекомендуется, чтобы был какой-то автоматический способ блокировки этого best practice, но хотя бы, чтобы это правило полностью исполнялось, требуется поправить policy, это отобразить, что имеется такое право, и как оно будет реализовано. И в какой-то внутренней инструкции.

[01:10:14]

Не справился, если ничего этого нет, и частично, если что-то из этого хотя бы одно есть. Важно. Человек может только при следующих случаях воспользоваться этим правом. В противном случае, пишем, когда оно не может быть исполнено. Точность данных оспаривается субъектом данных, в течение срока, который требуется контроллеру проверить реальность, правда ли эти данные точны или не точны. Обработка является неправомерной, и он хочет пока ограничить, чтобы разобраться в этом. Контроллеру больше не требуются эти данные для своих целей, но они требуются физлицу для исполнения защиты своего права в суде, либо где-то еще.

Проводилось автоматизированное принятие решения на основании обработки персональных данных, и субъект данных пытается понять, реально ли этот скоринг прошел. То есть после этой автоматизированной обработки мы правильно ли определили скоринговый балл, например, или нет. И мы блокируем данные. То есть по факту на момент разбирательства. В иных случаях данные не блокируются.

Далее. 1.21. Если мы данные исправили или удалили, или ограничили обработку, мы должны об этом уведомить человека. То есть, если мы по его запросу это сделали, то мы должны его по факту уведомить: мы сделали. Также у нас не исполняется, если в privacy policy или внутреннем документе это не отображено, это не исполняется. Исполняется, если хотя бы что-то одно есть, частично и полностью, если все есть. То есть, мы это публично отобразили. Но здесь какая-то инструкция, либо памятка о том, как это право внутри нашими сотрудниками реализуется по факту.

**То есть это должно быть указано, что в случае удаления ваших персональных данных, мы вам об этом сообщим?**

По вашему запросу, да. Либо без запроса, от нас это потребовал исполнительный орган. Хорошей практикой также считается, если у нас какой-то госорган получил доступ к данным, предупреждать об этом человека. По запросу: дать данные, – о'кей, мы тебя предупреждаем, у нас такой запрос запросили.

Далее. Выполнение права физлица на переносимость его персональных данных. Это выгрузка данных, но в машиночитаемом формате. Это у нас XML, JSON и CSV. То есть мы должны выгрузить и передать в ту компанию, в которую человек вас попросит. Например, я хочу перевести данные из Facebook в «ВКонтакте». Мы должны максимально ему помочь эти данные туда перенести. Очень похоже на выгрузку данных на DOS данных, помните, что первое смотрели. Получить список данных. Здесь то же самое, но еще мы помогаем все это дело перенести. Это право реализуется только тогда, когда у нас оснований для обработки, контракт с человеком, договор, или согласие. Во всех иных случаях мы не будем помогать это право реализовывать.

[01:15:12]

Переносится все. То есть здесь очень важно понять, что мы относим к персональным данным. Это может быть любая информация, но которая ценна для человека, для переноса. Очень простой пример, есть сервис «ЛитРес», знаете, для чтения книг. Там есть e-mail, или почта, аккаунт. Что еще может быть ценное, что мы должны перенести, что человеку будет полезно в дальнейшем?

**Студент:** Книги, которые он купил.

Книги, которые он купил. Да, что еще? Но это не персональные данные, но, в целом, да. Что еще?

**В «ЛитРес» что мы переносим из e-mail?**

Наоборот, что мы из «ЛитРес» выгружаем, помимо стандартной почты, указанной при регистрации?

**Имя, фамилию.**

Имя, фамилию. Что еще?

**Там при регистрации.**

Все, больше ничего.

**Страна, там.**

Страна, о'кей, что еще? Список книг на прочтение. Это может быть человеку полезным?

**Конечно, да.**

О'кей. Подборку книг на прочтение, то есть, есть свое, что вы сами ставите лайк – в будущем прочитаем. А есть публичный список, на который мы подписываемся. Тоже полезно? Полезно. Скорость чтения книг в год, аналитика. Нам это полезно? Я думаю, да, многие ставят целью, сколько книг мы читаем за месяц, за год, за полгода, типа, в день. И это не является персональными данными, но включить это в выгрузку мы это должны.

Не исполняется, если у нас это публично не заявлено, и у нас нет инструкции внутренней, как мы будем это право реализовывать. Частично что-то есть, и публично, то есть полностью исполняется, если у нас все о'кей, и публично мы заявили, и описали, как реализуется, и в каких случаях.

И есть внутренние какие-то инструкции о том, как нашим сотрудникам это право реализовывать. Что важно. Best practice считается, если у нас есть какой-то онлайн-кабинет у человека, чтобы это все было автоматизировано. Или даже не автоматизировано, то есть у нас есть e-mail человека, он вводит в форме, и на этот e-mail ему потом высылаются все данные о нем, грубо говоря. Это best practice. То есть за неисполнением best practice мы не считаем, что не выполнено. Это просто свободная воля компании. Но в рекомендации мы всегда прописываем, неважно, какой статус у этого требования.

Дальше. Выполнение права физлица на возражение обработки персональных данных. Это значит, что данные незаконно обрабатываются, то есть после сроков, либо без законных оснований, либо они неточные были изначально. Человек говорит: «Я хочу, чтобы они были уничтожены», то есть вы должны приостановить обработку этих данных и удалить их. То же самое, что и в прошлых пунктах, вы поняли, когда, что и как.

И финально, выполнение требований при автоматизированном индивидуальном принятии решении, включая профилирование. Что такое автоматизирование принятие решений, я вам говорил примерно, то есть скоринг, любая автоматическая обработка данных с каким-то результатом, который имеет правовые последствия. Отбор на учебу по баллам автоматически. Либо скоринг для получения кредита.

Если такое есть, то, первое, мы должны об этом публично указать в privacy policy и описать механизм, то есть общими словами, на основании каких данных и как происходит автоматизирование принятие решение, и что в итоге, то есть какие могут быть последствия от этого.

[01:20:12]

Человек не будет иметь права на оспаривание этой автоматизированной обработки, если у него нет договора. То есть для заключения договора, либо в момент договора требуется скоринг. То есть он понимает заранее, он не будет иметь права оспаривать эти решения, если он заранее об этом знал, по факту.

Вот этот скоринг разрешен одной из стран Евросоюза, или Евросоюзом, то есть смотрим законы и сайты надзорных органов, там все прописано. Или, если согласие явное, как вы понимаете, тогда это все законно.

Дальше. Есть профилирование. Это у нас в маркетинге. Есть профиль пользователя, и на основании этого профиля рекламу правильно показываем, либо товары правильно даем, либо скидку персональную определяем. Вот самое явное, это операторы сотовой связи видят, сколько мы разговариваем, что еще, и нам какие-то акции специальные дают. Не исполняется, если у нас не указано, например, что у компании нет обработки такой, но она не указала, что ее нет. Второе, у нас нет законных оснований на такую обработку, и она не указана публично. Частично исполняется, если хотя бы что-то указано, что у нас есть, но не описано. И полностью исполняется, если, первое, указано или что у нас ее нет, или указано, что она у нас есть, написано, как это все работает. Описано правовое основание, и описано право на возражение такой автоматизированной обработки.

Вопросы? Все. Давайте передохнем.

**[01:22:48][Конец записи]**

**[00:00:00][Начало записи]**

**Преподаватель:** У нас это будет записываться, но если в политике о том, что для исполнения своих прав, ваших прав для их реализации, нам могут потребоваться ваши дополнительные данные, чтобы вас идентифицировать. Если вы их не будете предоставлять, в таком случае, мы не сможем реализовать то ваше право, за которым вы обратились.

Далее. 2.3. Выполнение требований по защите данных по умолчанию и при проектировании. На английском это privacy by design и privacy by default. Что такое privacy by design. Это когда мы проектируем новую систему, где будут данные, сервис, внутренняя информационная система, где будут данные, либо процесс обработки данных, как-то новый процесс, новая цель, процесс, либо мы их меняем, либо что-то еще, мы должны провести процедуру оценки рисков для физлица. То есть сразу проектируем, у нас техническое задание. Мы его смотрим. Проводим процедуру DPIA, это Data Protection, то есть анализ рисков для физлиц. Если видим, что, о'кей, новые риски появляются, сразу делаем какие-то контроли, то есть меры по защите, проектируем. И теперь с этими мерами защиты безопасность защиты данных при проектировании реализовывается.

Privacy by default. Это что стандартно всегда при проектировании, при разработке выполняются следующие условия: обезличивание персональных данных. Стараемся максимально обезличить сразу, по дефолту. Или псевдоминимизация этих персональных данных. Что это такое? Это когда у нас есть база данных, в ней несколько таблиц. У нас таблицы, там ID имя, ID фамилия, ID e-mail, понимаете. Почитайте отдельно про псевдоминимизацию в интернете. Там об этом всем написано, как это может быть реализовано. И шифрование данных любыми способами шифрования.

И далее минимизация данных. Мы должны стараться при изменении, по умолчанию, бла-бла-бла, минимизировать всеми силами состав данных, который требуется для целей обработки данных в новом процессе, либо в изменяемом, либо как сейчас, в уже имеющемся таком процессе. Вопросы здесь?

Не исполняется, если у организации эти два процесса разных, понимаете, privacy by design и privacy by default нет этого процесса описанного, и, вообще, даже устного, понятийного. Тогда это не исполняется. Если же у нас что-то частично указывается, где-то отображено, какие-то риски физлиц определяются, например, в российской модели угроз по нашему закону, частично, или какие-то меры защиты принимаются хотя бы. Полностью исполняется, если это внедрено как процессы, два процесса, и они исполняются. И есть документ, где это зафиксировано.

Пункт 2.4. Исполнение требований по совместной обработке персональных данных с другими контроллерами. Например, в одной цели, мы и Google-аналитик, совместный с контроллером, то, что мы свое собираем, а это их софт, ни сами функционал закладывают в него, значит, он нужен для этих целей. Поэтому совместные контроллеры. Надо смотреть договор с Google, должно быть это прописано. И мы обязательно должны это указать в privacy policy, если такой имеется.

[00:05:05]

Не исполняется, но если у нас в privacy policy не отображено, что есть совместные контроллеры, хотя они имеются. И с совместными контроллерами не заключен договор о совместной проработке персональных данных, или соглашение. Частично исполняется, если у нас, например, хоть что-то из этого имеется. Например, есть соглашение, но в политике не отражено. И полностью отражено в политике, и есть соглашение.

Наличие представителей на территории Евросоюза. Если компания находится за пределами Евросоюза, или даже за пределами Европы, вот этого единого экономического пространства, но данные обрабатывает там отдаленно как-то. Примеры – у нее есть удаленный магазин, либо сервис, либо она делает мероприятия удаленно и данные собирает. Либо компания из Евросоюза получает данные на обработку в Россию, то есть она данные обрабатывает тех людей, которые физически находятся на территории Евросоюза, и у нее нет своих офисов там, она должна назначить там представителя по DGPR. Это физлицо или юрлицо.

Если у организации есть филиал или представительство, может быть такое представительство, то факт того, что есть представитель, это документ из их органа, что, о'кей, представительство такой-то компании. Это у нас так сейчас с Россией РИА «Новости», или «Россия сегодня». Там у них есть представительство, и мы смотрим, какие документы есть, и дальше одно из них назначаем. Если там филиал, то во внутренних документах это должно отображаться, о'кей, что там реально есть филиал, или обособленное подразделение.

Далее, исходя из этого, мы должны назначить туда, или наш офис там, который законно основан там, то есть это или представительство, или филиал, или обособленное подразделение. Либо это внешняя организация или физлицо, которое будет наши интересы там представлять. С таким лицом должен быть заключен договор на услуги представительства, если это внешняя компания за деньги. Обязательные требования к представителю, это то, что он, первое, предоставляет информацию по запросу физлиц или регуляторов по персональным данным, или контрагентам. Он также несет ответственность за нарушение закона контроллером, например, из России.

Далее. Если у компании много офисов или дочерних предприятий, или представительств, или обособленных подразделений, или филиалов на территории Евросоюза, она должна выбрать одно основное. Опять же, если это на территории разных стран Евросоюза. Как оно определяется. Если через этот филиал идет управление, координация всех остальных. Вы должны такое выбрать или выявить. Если такого нет, просто посоветуйтесь с заказчиком тогда. Не исполняется, если просто нет представительства вообще.

[00:10:08]

Второе, исполняется частично, если оно есть, или они есть, но не назначен, договор не заключен и не выбрано основное. Мы или/или, потому что, если у нас внешняя организация будет нашим представителем, то там просто договор. И выполняется полностью, если у нас там представительство и с ним заключен договор, выбрано основное представительство, если у нас несколько вариантов есть. Вопросы?

**Студентка:** По поводу договора, он как-то должен в открытом доступе где-то?..

**Преподаватель:** Он только по запросу регулятора будет предоставляться. Договор должен быть двуязычным, например, если у нас представитель внешний из Германии, а мы – российская компания. Это делается обычно две таблички в договоре (два столбца). С левой стороны немецкая версия, с правой стороны русская версия.

Дальше. Поручение персональных данных на обработку обработчику или процессору, policy PR. То есть, есть те, кто в наших интересах будет обрабатывать персональные данные на обработку. Например, мы поручаем бухгалтерские компании вести бухучет наших работников. Либо, мы поручаем маркетинговому агентству в наших целях обрабатывать персональные данные. С такими организациями должно быть заключено Data Processing Agreement, вообще, без разницы, как он будет называться, на самом деле, там как его только не называют.

С ним должен быть заключен договор, который должен быть подписан в бумажном или в электронном виде. Что должно быть в этом документе. Гарантии того, что процессор обрабатывает персональные данные только на основании документально подтвержденных распоряжений контроллера, в том числе, в отношении передачи данных третьей стране или международной организации, если это надо для исполнения договора. Это значит, что в этом договоре, либо в этом документе должно быть прописано, что это именно контроллер дает распоряжение этому процессору. Если, например, будет в договоре, что исполнитель сам обязуется думать, как там проводить маркетинг, то они совместно с контроллером, а не схема контроллер-процессор. Поняли?

**Студентка:** Нет.

**Преподаватель:** Хорошо, иначе скажу. Грубо говоря, я даю бухгалтерии, говорю: о'кей, ты должна сделать вот это, вот это, вот это, внешне. Есть четкая инструкция, четкое распоряжение, что мне делать. Если в договоре этого нет, значит, та сторона сама определяет цели обработки, их состав свойства обработки. Раз она определяет, значит, она тоже контроллер. Если мы сами ставим цель, что делать, как делать, какие данные, – мы контроллер, и даем, как процессору, точно по нашей инструкции это все исполнять. Если этой инструкции нет, краткой в договоре, то та сторона тоже имеет свои законные основания на обработку. Значит, она тоже контроллер этих данных, что мы поручили. Понимаете?

**Студентка:** А им нужно как-то отчитываться о том, какой они выбрали?..

**Преподаватель:** Да. До того, как мы с ними заключаем, мы говорим: о'кей, коллеги, мы думаем, что вы наш процессор. На самом деле, нет, мы хотим быть контроллером. Это все вопрос обсуждения с ними. Даже с крупными компаниями, как Google, или Facebook.

Далее. Если они процессор, и мы с ними договорились, то в таком документы должны быть прописаны гарантии того, что только в этих целях данные будут обрабатываться, только в тех целях, которые нам контроллер поручил их обрабатывать.

Дальше, гарантии этого процессора. Соблюдать конфиденциальность и целостность данных, и какие-то гарантии, то есть список того, что организации применяют, чтобы обеспечить защиту персональных данных.

[00:15:14]

Дальше. Если процессор еще будет привлекать субпроцессоров, то есть все те стороны, которые хостинг-провайдер, другие, кому данные, так или иначе, могут передаваться для исполнения этого поручения, он должен, во-первых, их отразить, и выстроить правильную структуру того, что он заранее будет предупреждать оператора, контроллера о том, что мы хотим привлечь вот эту сторону. То есть уже после заключения этого договора. То есть мы должны сменить хостинг-провайдера, мы должны заранее, опять же сроки не регулируются законом, можем сами заранее определить, и уведомить контроллера об этом.

Какие способы уведомлений. Первое, это каждый раз получать согласие контроллера на то, чтобы привлечь нового субпроцессора, либо же изначально в договоре прописать, что контроллер дает полное решающее согласие, но только в том случае, либо при добавлении или изменении списка субпроцессоров, он заранее будет об этом уведомляться. То есть контроллер, может сказать: нет, ты хочешь новых хостинг-провайдеров в России, я не хочу.

Информация о том, что процессор будет помогать контроллеру реализовывать права физлиц, если эти данные обрабатывает процессор. Например, поступает запрос на удаление персональных данных, и мы обязаны эти данные удалить не только в наших системах, но и в системах процессора. Мы должны уведомить об этом, либо там инструменты программные, как их автоматом удалить.

Далее. О том, что заказчик исполняет DPIA и делает защиту данных, что у него началось DPO на процессоры, если требуется. И он может передать нам свое DPIA – Data Protection Impact Analysis, то есть оценку рисков. Я говорю: о'кей, смотри, я тебе передаю свои данные, но мне для внутренней документации требуется твоя оценка рисков. Дай мне, пожалуйста. И дай мне контактное лицо, с кем мне общаться privacy.

Дальше. Если договор перестает действовать, то гарантии того, что данные будут удалены, и нам переданы в полном объеме. То есть, сначала нам переданы процессором обратно, и потом удалены.

Дальше. Гарантии того, что мы можем провести аудит с включением третьей стороны, того, что, действительно, процессором соблюдаются пункты данные DPIA. Это можно много всего написать в нем, то есть мы должны понять, что реально ли эта компания все это соблюдает, и все это может, что она написала в этом договоре. Но обязательно до этого мы должны за 30 дней уведомить компанию об этом. То есть опять же, с разрешения процессора мы должны это делать. Право там это есть, но срок и дату мы с ним обсуждаем. Опять же, не исполняется, если ничего не заключено. Исполняется частично, если что-то из этого там указано, и полностью, если по всем этим правилам документ утвержден письменно или электронно.

Опять же, если что-то изменяется в DPIA со стороны процессора, кроме списка субпроцессоров, нужно об этом незамедлительно сообщить, – об утечках данных, о том, что свои цели появились в обработке этих данных, по законодательству, и так далее. Он должен об этом сообщить контроллеру, и это должно быть прописано в DPIA.

[00:20:12]

**Студентка:** Контроль только риски? Там же по поводу рисков шла речь, а тут вы говорите, что если появились какие-то лишние цели.

**Преподаватель:** Смотри, первое. До заключения контракта мы говорим: о'кей, мы готовы тебе данные передавать, но нам для своей внутренней документации надо понимать, как ты данные защищаешь, дай мне свой DPIA, это по рискам. Он должен дать. Далее. Список субпроцессоров, кому он дальше передает данные, тоже должен дать. Если у нас изменяется список процессоров, субпроцессоров, я сказал, что делать, – там или каждый раз брать согласие, либо просто его уведомлять заранее об этом.

Если же меняются, например, меры защиты, он говорит: мы теперь больше не можем такие меры защиты обеспечивать. Бывает же все у компании. Или, мы переезжаем в другую страну, или появилась трансграничная передача у процессора. Либо же у него появилась своя цель в обработке данных. Он говорит: о'кей, в ваших целях будут данные обрабатывать, но у меня еще свои цели появились, я вас об этом уведомляю. Например, вышел закон о том, что все интернет-магазины должны передавать данные в госорган. Это не моя прихоть, это закон вышел, поэтому я вас об этом предупреждаю. Или была утечка данных. Мы обязаны об этом предупредить, данных, в том числе, тех, которые вы нам передали на обработку. Поняли?

Далее. Требования по ограничению цели обработки данных только списки, обработки в иных целях, которые установлены правом ЕС или же страны, или государств-членов ЕС. То есть, если у нас есть закон Яровой, мы не можем сказать, что это законное основание. Но мы должны его как-то переформатировать. Опять же, если этого нет, то ищем законные основания и требование такое должно быть в DPIA. То есть не исполняются требования – нет, исполняются частично – там оно имеется, но какое-то кривое, корявое. И исполняется, – оно имеется полностью и прописано в DPA.

Дальше. Наведение учета обработки персональных данных. В законе прописано, что это должны делать только некоторые компании, если у них больше 250 работников, но я считаю, что должны делать все компании для прозрачности. Что должно быть там указано, вы можете увидеть в этом пункте, там все описано. Документ называется Data flow date inventory. Абсолютно неважно, как вы его назовете, в какой форме он будет, главное, что это должно быть описано. Тут написаны, что это имя и контакты данных контроллером взятые у процессора, и или DPO, там все это есть.

В ходе обработки персональных данных физлиц, и также по-процессно. Один процесс, пишем все полностью о нем. И так далее. Это очень похоже на privacy notice, но только расширенно пишем по каждому процесс абсолютно. То есть там обобщенно, там идет привязка по категориям физлиц, здесь – по процессам, по целям. Какие отделы участвуют, для чего, все цели в данном процессе. Туда передается, и DPIA по ним указывается, проводился или нет. То есть здесь я все вам максимально описал, вы можете это все увидеть. Опять же, если даже никаких законов не требуется, то есть у них меньше 250-ти, мы все равно в рекомендации пишем, что для best practice нужно все-таки документ прописать.

Дальше. Сотрудничество с надзорным органом. Надзорный орган пишет запросы, в течение 30 дней контроллер обязан отреагировать и прислать всю запрошенную информацию, либо нормативный ответ. Является неисполнением, если ничего такого нет, то есть процедура формально или устно не определена. Частичное исполнение, если у нас есть хотя бы или устная или письменная процедура такого реагирования. И полностью, что есть письменная форма, она такая же, как реальная. Понимаете? То есть бывает такое, что в документе написано одно, а люди делают по-другому. Все это совпадает.

[00:25:17]

Далее. 2.10. Обеспечение безопасности персональных данных. Опять же, здесь самое главное, что очень похоже на предыдущие пункты, что есть процедуры защиты, и есть документ, который описывает эти методы защиты. Это или IT security policy, либо Data protection policy, либо Security policy. Для определения списка угроз можно здесь DPIA проводить, то есть процедуру Data Protection Impact Analysis. Не исполняется, если ничего нет, точнее, ни средств защиты, ни документирования. Исполняется частично, если DPIA проведен, но не внедрено, если просто есть средства защиты, или есть просто какой-то формальный документ, который описывает то, что компания должна делать, но по факту не делает. Полностью, – есть процедура, есть документ, средства защиты, проведена DPIA.

2.11. Уведомление надзорного органа об утечке персональных данных. Если мы выявили инцидент, должна быть регламентирована процедура, что в течение 72 часов мы должны определить риск того, это высокий риск этой утечки для субъектов данных или нет. Например, просто e-mail утек, это не страшно. Просто список e-mail, там e-mail и пароль, или e-mail и, знаете, была сеть для любовников, не помню, как она называлась. Была такая. Если там e-mail течет, там уже, понимаете, высокий риск. Сразу понятно. Это была единственная в мире утечка, но которая привела к известным фактам, к смерти человека, то есть он из окна выкинулся. Там узнали, с кем он спал, или с кем он изменял. Или женам изменял, я не знаю, чего там было.

Если понятно, что риск высокий, пишем в течение 72 часов, как мы инцидент определили, то есть мы его выявили. Это может быть, понятно, и СМИ. То есть, мы: о! А что, была утечка из СМИ? Определили, у себя посмотрели, и в течение 72 часов должны отреагировать на момент того, как мы узнали об этом из СМИ. У каждого регулятора в странах ЕС есть онлайн-форма, почти у всех, где можно заявить об инциденте.

Далее. Не исполняется, если нет вообще никакой процедуры, ни формальной, ни описанной. Исполняется частично, если это кратко где-то написано, или есть хоть формально, просто ее там нет. И полностью исполняется, если есть формальная процедура, она совпадает тому, что написано бывает в документе, и она исполняется. То есть, если уже в компании были утечки, вы проверяете, как она реагировала на них и согласно тому, что у них написано в документе.

2.12. Если риск там высокий при утечке данных, опять же, под утечкой данных я понимаю нарушение конфиденциальности или целостности персональных данных, понимаете? То есть я это называют Data breach, или утечка персональных данных, для простоты. Если риск высокий, мы должны принять меры на минимизацию рисков для физлиц. Например, сбросить всем пароли, и непосредственно как-то минимизировать, или бэкап надо там восстановить.

Опять же, инцидент может быть, как внешним, так и внутренним. У нас что-то поломалось, целостность данных нарушена. И написать потом письмо физлицам, чьи данные могли пострадать. Опять же, мы не всегда имеем возможность определить, из какой страны человек. Можно работать во всем мире, как у нас, например, «Битрикс24», наш клиент. И не понимаешь, кто именно, с какой стороны. Поэтому пишем какой-то группе, что был такой инцидент, он мог повлиять на ваши данные, вот что мы сделали. Если есть вопросы, чтобы риск минимизировать для вас, пожалуйста, если есть опасения и вопросы, напишите нам, вот наши контакты.

[00:30:20]

Это обязательное условие. Еще к пункту 2.11. Если у нас есть утечка, мы должны также вести для полного учета реестр утечек. Когда, кто определил, как определил, в чем она заключалась, что мы сделали, какой риск – высокий или низкий, почему там такой высокий или низкий, что мы сделали для минимизации рисков для физлиц, когда уведомили людей, когда уведомили госорганы – дата, время.

Следующий пункт 2.13. Проведение оценки DPIA. Она требуется не для всех. Давайте я вам сейчас прочитаю, просто там очень много заметок, я наизусть не помню...

Называется оценка воздействия защиты данных. Вообще, оценка здесь она конфиденциальность. Это DPIA, это Data Protection Impact Analysis. Не путайте DPIA и DPA. Data Processing Agreement – это поручение на обработку, DPA, и Data Protection Impact Analysis, это DPIA. Очень часто это можно перепутать при разговоре.

В каких случаях она требуется. Систематическая и всесторонняя оценка личных аспектов, то есть профилирование, либо автоматизированная обработка есть с принятием решений, имеющих правовые последствия, то обязательно надо проводить. Далее. Обработка персональных данных специальных категорий, чувствительных категорий в большом объеме. Что имеется в виду под масштабом и объемами. На территории одного города все данные, там львиная доля данных. То есть на территории региона, города, поселения, округа, страны, либо Европа. Должны сами все это определить. И опять же, специальных категорий данных, то есть чувствительных данных. То есть это много что затрагивает по территориальному признаку.

Дальше. Есть систематический мониторинг общедоступной области. То есть мы здесь мониторим очень большое количество физлиц. Например, у нас очень популярное приложение, им пользуются в Европе, это приложение по бегу, и мы отслеживаем геолокацию. Постоянный мониторинг там действует, и камеры слежения. Либо датчик GPS, либо аналитика там постоянно снимается, как у Apple. Это все относится сюда. Это что прописано в законе.

Есть еще рекомендации WUP-29 про DPIA, очень интересная, кстати, сейчас я вам расскажу. Либо проводится, если есть высокий риск. Но высокий риск должен соответствовать минимум двум, что высокий риск будет, если обработка соответствует минимум двум вышеуказанным критериям.

[00:35:05]

Первое, есть прогнозирование или профилирование маркетинговый, финансовый, скоринг KYC, и генетический анализ. KYC знаете что это такое? В Европе и в других разных странах, Штатах, просто так прийти в банк и положить деньги на депозит не получится. В России – спокойно, да, конечно. А там проверяют, откуда у тебя получен такой капитал, законность того, что ты эти деньги где-то не своровал.

Далее. Автоматизированное принятие решений на основании обработки данных, или приводящие к юридическим последствиям, или оказывающих серьезное воздействие на физлиц. То есть это могут быть не юридические последствия, но затронуты какие-то аспекты жизни физлица. Например, на основании нашего теста ты даун, бляха-муха, но это серьезные последствия. Системный мониторинг данных, в том числе, общедоступных. Далее, обработка специальных категорий данных. Опять же, ничего не сказано про общее в большом масштабе и объеме. Просто оно имеется.

Далее. Любая обработка данных в больших масштабах, в масштабах города, района, области, страны. При этом учитывается, как долго не обрабатывается в большом масштабе, в большом объеме, и какой состав данных. Это могут быть даже не специальные данные, но в большом объеме и долго хранятся, попадают.

Обработка в разных целях и с другим контроллером. То есть, есть совместные контроллеры. Обработка данных, защищаемых на категории субъектов данных. Кто это? Психбольные, дети, пациенты больниц, пожилые, беженцы, жертвы насилия и люди, которые просили убежище. Если у нас есть такие категории, о'кей.

Применяются новые технологии или инновационные формы обработки персональных данных. Например, это интернет-устройства, датчики разные. Это Face ID, и иная биометрическая идентификация. То есть любые какие-то новые процессы, либо что-то еще, новые технологии. Надо проводить. Если два пункта из этих совпадают, у нас высокие риски, мы должны проводить DPIA. У DPIA есть определенная форма. То есть, как понять, что DPIA, первое, оно должно быть, если мы приняли, что по пунктам, оно должно быть, либо где-то из этого списка, что я сейчас перечислил, а у компании ее нет. Далее, второе, DPIA проведено, но проведено с ошибками. Третье, DPIA проведено, проводится регулярно, и пересматривается без ошибок.

Если мы работаем в секторе B2B, то есть мы поставляем, например, мы компания «Битрикс», мы предоставляем веб-сервис для кооперативной работы над проектами. То есть нам компания дает данные своих работников. И этой компании требуется сделать свой DPIA, вести учет всех процессов, и как в этих процессах DPIA будет проведен. Они один процесс нам делегируют, и на это просят DPIA. Мы не хотим давать наш внутренний DPIA большой, но хотим дать поменьше. В DPIA описана каждая угроза и гарантирован ответ, в общем, она актуальна или нет, почему да или почему нет. Здесь должны просто сказать: да, нет, да, нет. То есть сокращенная форма им предоставляется.

[00:40:02]

После того, как мы выявили, например, высокий риск в каких-то пунктах, применили инновационные и технические меры, направленные на снижение рисков, это контроль доступа, средства защиты. Проводим снова DPIA, смотрим, помогли ли эти средства защиты снятию рисков. И когда он снижен, то все, о'кей. Вопросы?

Я понимаю, что это сложновато сходу определять, но я надеюсь, что в дальнейшем по этому обучению вы сможете сейчас сами хоть как-то, хоть левой ногой проводить эту оценку соответствия с рекомендациями, и потом можно будет работать по живому.

Далее. Назначение инспекторов по защите персональных данных. Здесь написаны случаи, когда они должны быть, прямо выписаны, я не буду сейчас это рассказывать вам. Но если компания не попадает ни под один из этих пунктов, что здесь перечислены, в этой статье, то по рекомендации WUP-29 надо назначить ответственного хотя бы. Если даже закон в значительной степени не требует от вас этого человека, то назначьте какого-то другого, кто будет нести эту ответственность, это исполнять.

Это очень важно почему? В некоторых странах внедрены сертификации определенной DPO, например, в Испании по их стандарту. Если человек не прошел эту сертификацию, то он не может оказывать услуги DPO. А если по закону компании не требуется ответственный по DPO, он может быть без сертификации, поэтому обязательно смотрим DPO тот закон, который есть в той стране, где мы смотрим. Потому что они под себя этот закон могут дорабатывать. Там же, в этом пункте я бы дописал, какие обязанности должны быть у DPO. Или вы можете их просто посмотреть в трех статьях – 37, 38 и 39.

Не исполняется, если у них он должен быть, но его нет. Исполняется частично, если есть инструкция, но не человека, то есть, есть инструкция должностная DPO, но нет человека. Или если человек есть, а на инструкции его нет. Очень важно DPO, если он официально назначается на должность, он может быть и внутренним, и внешним. То есть это либо наш работник отдельный, которому мы платим деньги, либо это внешняя компания, которая нам предоставляет своего человека. Там не должно быть конфликта интересов.

То есть, что он нам подотчетен, и действует в наших интересах. Он не должен смотреть на требования бизнеса, на то, что бизнес исполняет требования GDPR, и не должен бизнес покрывать. Например, бизнес говорит: у нас есть серая обработка, ты об этом ничего не знаешь, и должен это пропустить. Это запрещено. И полностью исполняется, если есть человек, он может работать на этой должности по законодательству той страны, нет конфликта интересов, и есть инструкция, то это выполняется полностью. И DPO должен быть у компании. Если у компании DPO не требуется, то VNT пишем, – не требует выполнения.

И последний пункт, 2.16, это выполнение требований при передаче персональных данных в третьи страны. Если мы передаем данные в хостинг, либо подрядчикам, поставщикам, либо процессорам за рубеж, или мы сами находимся за рубежом, есть три возможных способа передать данные в Россию. Первое, с согласия физлица. Второе, если мы гарантируем, что у нас приняты стандартные контракты и условия. Это standard contracts and conditions. Вы можете в интернете погуглить, в этом пункте, я их указал.

[00:45:17]

Они стандартные. То есть мы гарантии оттуда записываем в privacy policy, и такие документы подписываем со всеми нашими поставщиками, кто на территории стран не Евросоюза, то есть которые не обеспечивают эту защиту, как вы понимаете. Если мы в России и дальше кому-то эти данные юрлицам передаем в России, мы обязаны эти контрактные условия заключить. Они стандартные, их нельзя менять. Это важно, потому что эти шаблоны утверждены Еврокомиссией.

И третий способ, это обязательные корпоративные условия. Иначе они прописываются Binding Corporate Rules, BCR. К ним есть определенные требования, к такому документы, вы его должны посмотреть в законе, я написал в какой статье. Зачем нужен этот документ? Если у нас международная компания, и у нас есть глобальные системы, данные со всех стран передаются, то есть непрерывно, то пишется по этому пункту GDPR этот документ, внутри согласовывается. Дальше он согласовывается с нашим главным регулятором на территории Евросоюза. Принимается всеми, то есть все лица в мире этой компании подписывают документ, и все. Им не надо между собой какие-то документы подписывать, потому что регулятор согласовал, какие у нас правила, и они исполняются. То есть мы просто пишем в privacy notice, что есть такой BCR, мы готовы вам его предоставить и показать.

Компания исполняет требования, если у нее полностью все или что-то из этого принимается. Не исполняет, если не принимается. И частично, если частично исполняется. Например, если мы при передаче, то есть европейской компании, но передавать кому-то в России. Но у нас с ними не заключено. С другими странами у нас все законно передается. И согласие есть, и стандарты, construction close на BCR. А по одному нет. Значит, по одному контрагенту или процессу нет. Значит, пишем – частично и полностью, если у нас чем-то из этого все перекрыто. Понимаете? Все.

**Студентка:** У меня вопрос. Какой алгоритм составления этой оценки? То есть мы отталкиваемся от политики, которую мы рассматриваем, или мы отталкиваемся от регламента?

**Преподаватель:** Первое, так как у вас нет всей информации о тех компаниях, что вы можете сделать. Как получить дополнительную информацию? Написать им запрос о том, что вы являетесь клиентом, либо как-то с ними работаете. Можете сказать, как вы данные обрабатываете. То есть где почитать об обработке, вдруг какие-то документы, которые они скидывают, и которые явно не видны. Это первое. Второе, самим полазить по их сайту, сайтам.

Третье, додумать, ну, а что делать? У вас нет возможности, но вы же не можете сейчас пойти к нашему заказчику, сменить данные и на него сделать. Поэтому вы должны придумать что-то. Я имею в виду, написать запрос и самим поискать. Потому что времени у вас вагон еще. То есть что-то, что можно исправить в policy. Мы записывали что-то выявить, это вот давайте выявим. Давайте хотя бы то, что связано с privacy policy мы выявим.

Дальше, что еще. На территории той страны, где работает компания, регулятор выкладывает списки тех, у кого приняты BCR, стандартные корпоративные условия. Это можно там посмотреть, то есть компания приняла или нет. Дальше, DPO также должны быть зарегистрированы у этого главного надзорного органа. Там есть списки, поэтому тоже можно их посмотреть.

**Студентка:** Это зависит от того, есть ли у них сертификация или нет?

[00:49:55]

**Преподаватель:** У каждого по-разному. Неважно. Например, в Испании ты не сможешь зарегистрироваться, если нет сертификации. Но я с вас не требую этого сейчас, потому что вам нужно много опыта, чтобы все это узнать и посмотреть все страны, все законодательства. Вопросы? У вас есть понимание шагов своих следующих?

**Студентка:** Да. Нам нужно закончить то, что мы делали до этого, правильно написать...

**[00:50:32][Конец записи]**