**OVERVIEW**

1. США, в отличие от ЕС, используют секторальный подход, сочетающий законодательство, регулирование и саморегулирование. Министерство торговли, чтобы урегулировать существующие различия в обеспечении конфиденциальности, выпускают принципы Privacy Shield (защита конфиденциальности), включая Supplemental (дополнительные) принципы, обобщенно называемые "Принципы" для обеспечения Международной торговли. Принципы были разработаны совместно, чтобы облегчить торговлю между США и ЕС. Они предназначены исключительно для организаций в США, работающими с ПДн от ЕС. Принципы не влияют на существующие положения, имплементирующие директиву 95/46/ЕС Европейского союза. Принципы не ограничивают обязательства по конфиденциальности, которые применяются в соответствии с законодательством США.

2. Чтобы полагаться на Privacy Shield организация должна самостоятельно подтвердить соблюдение принципов Министерству торговли или его назначенному лицу. Для эффективного соблюдения требований необходимо:

    а) самостоятельно сертифицироваться. Чтобы вступить в Privacy Shield, организация должна быть субъектом проверки в рамках полномочий FTC, Министерства транспорта или другого подзаконного органа;

    б) публично заявить о соблюдении Принципов;

    в) публично раскрыть Privacy Policy в соответствии с Принципами;

    г) Полностью выполнить их.

Невыполнение подлежит исполнению в соответствии с разделом 5 ФЗ о торговой комиссии, запрещающий недобросовестные и вводящие в заблуждение действия.

3. Министерство торговли ведет список организаций США, которые прошли самосертификацию и заявили соблюдении Принципов (Список Privacy Shield). Преимущества Privacy Shield гарантируются с даты включения в список. Министерство будет удалять организации из списка Privacy Shield при добровольном выходе, не соблюдении Принципов или прекращения подаче ежегодной повторной сертификации. Удаление организации из списка Privacy Shield означает прекращения получения преимуществ. Организация продолжает применять Принципы к личной информации, полученной во время участия в Privacy Shield, и подтверждать это на ежегодной основе, пока она сохраняет такую информацию; в противном случае, необходимо вернуть или удалить информацию или обеспечить защиту возможными средствами.

4. Министерство ведет четкий список организаций США, которые ранее прошли самосертификацию в Министерстве, но которые были удалены из списка Privacy Shield, и предупреждает об этом. Такие организации не могут претендовать на соответствие Privacy Shield и должны избегать любых заявлений или вводящей в заблуждение практики, подразумевающей, что они участвуют в Privacy Shield; Организация, вводящая в заблуждение, может быть подвергнута принудительным действиям со стороны FTC или других компетентных органов;

5. Соблюдение этих Принципов может быть ограничено:

    а) в той мере, в какой это необходимо для удовлетворения требований национальной безопасности, общественных интересов или правоохранительных требований;

    b) по закону, постановлением правительства или прецедентным правом, которое создает коллизии обязательств или явное разрешение, при условии, что при осуществлении любого такого разрешения организация может продемонстрировать, что ее несоблюдение Принципов ограничено в той мере, в какой это необходимо.

    С) если директива или законодательство государств-членов допускают исключения или отступления, при условии, что такие исключения или отступления применяются в сопоставимых условиях.

   В случае ограничения соблюдения Принципов необходимо указывать в своей Privacy Policy, где происходит исключения из Принципов, разрешенных в подпункте (b), на регулярной основе. По той же причине, когда ограничение допустимо, ожидается выбор наиболее возможной полной защиты.

6. Организации обязаны применять Принципы ко всем персональным данным, передаваемым с использованием Privacy Shield, после входа в Privacy Shield.  Организация, распространяющая Privacy Shield на информацию о людских ресурсах организации, переданные из ЕС для использования в трудовых отношениях, должна указать, когда она самосертифицируется в министерстве по требованиям, изложенным в дополнительных принципах самосертификации.

7. Законодательство США будет применяться к вопросам толкования и соблюдения Принципов и соответствующей Privacy Policy организациями Privacy Shield, за исключением случаев, когда такие организации обязались сотрудничать с европейскими органами по защите данных (“DPAs”).  Если не указано иное, все положения принципов применяются там, где они уместны.

8. Определения:

    a. “Персональные данные” и "личная информация" - это данные об идентифицированном или идентифицируемом физическом лице, которые входят в сферу действия директивы, полученные организацией в США от ЕС и записанные в любой форме.

    b. "Обработка" персональных данных - любая операция или комплекс операций, которые выполняются с использованием персональных данных, будь то автоматизированными средствами, такими как сбор, запись, организация, хранение, корректировка или изменение, поиск, консультирование, использование, раскрытие или распространение, а также стирание или уничтожение.

    с. “Контроллер” - лицо или организацию, которое самостоятельно или совместно с другими определяет цели и средства обработки персональных данных.

9. Датой вступления в силу принципов является дата окончательного утверждения определения адекватности Европейской комиссией.

**notice**

а. Организация должна информировать людей о:

    1. своем участии в Privacy Shield и предоставить ссылку или веб-адрес на список Privacy Shield;

    2. типах личных данных, которые собираются и, при необходимости, подразделения или дочерние организации, придерживаясь Принципов;

    3. своём обязательство в соответствии с Принципами, связаное со всеми персональными данными, полученными от ЕС в соответствии с Privacy Sield;

    4. целях, для которых она собирает и использует личную информацию;

    5. том, как связаться с организацией с любыми запросами или жалобами, включая любое соответствующее учреждение в ЕС, которое может ответить на такие запросы или жалобы;

    6. типе или личносте третьих лиц, которым она раскрывает личную информацию, и цели, для которых она это делает;

    7. правах физических лиц на доступ к своим личным данным;

    8. выборе и средствах, которые организация предлагает физическим лицам для ограничения использования и раскрытия их персональных данных;

    9. независимом органе по разрешению споров, назначенном для рассмотрения жалоб и предоставления соответствующих бесплатных средств правовой защиты отдельному лицу, и являющийся:

        1) группе, учрежденной DPAs,

        2) альтернативном поставщике услуг по разрешению споров, базирующимся в ЕС, или

        3) альтернативном поставщике услуг по разрешению споров, базирующимся в США.

    10. Том, что она является субъектом следственных и исполнительных полномочий FTC, Министерства транспорта или любого другого уполномоченного статутного органа США,

    11. возможностях, при определенных условиях, для физического лица ссылаться на обязательный арбитраж,

    12. требованиях раскрывать личную информацию в ответ на законные запросы государственных органов, в том числе для удовлетворения требований национальной безопасности или правоохранительных органов, и

    13. его ответственности в случаях последующей передачи третьим лицам.

b. Это уведомление должно быть представлено четким и понятным языком, при первом обращении физического лица или как можно скорее после обращения, но в любом случае до того, как организация использует такую информацию для целей, отличных от первоначальных или раскрытия ее впервые третьей стороне.

**CHOICE**

    a. Организация должна предоставить физическим лицам возможность выбрать (отказаться), может ли их личная информация (i) быть раскрыта третьей стороне или (ii) использоваться для целей, которые существенно отличаются от первоначальных целей или впоследствии разрешенных им. Физические лица должны быть обеспечены четкими, понятным и легко доступными механизмами для этого.

    б. В дополнение к предыдущему параграфу, выбор предоставлять не требуется, когда раскрытие информации третьим лицам происходит для выполнения задач от имени или по поручению в качестве агента при заключенном договоре с ним.

    c. Для чувствительной категории информации (т. е. медицинских записей или состояние здоровья, расового или этнического происхождения, политическая принадлежность, религиозных или философских убеждений, членства в профсоюзах или информации с указанием половой жизни лица) необходимо получить от отдельных лиц прямое согласие, если такая информация должна быть (i) раскрыта третьей стороне или (ii) использована для целей, отличных от первоначальных или разрешенных им впоследствии. Кроме того, организация должна рассматривать информацию, полученную от третьей стороны, как чувствительную, если третья сторона идентифицирует и рассматривает ее как чувствительную.

**ACCOUNTABILITY FOR ONWARD TRANSFER**

    a. Для передачи личной информации третьей стороне, действующей в качестве контролера, организации должны соблюдать Принципы Notice и Choise. Организации должны также заключить договор с контролером третьей стороны, который предусматривает обработку только в конкретных целях и в согласии с физическим лицом, при уровне защиты, как и в Принципах, с уведомлением при отсутствии такой возможности. В договоре предусматривается, что при вынесении такого определения контролер третьей стороны прекращает обработку или принимает меры по исправлению положения.

    б. На передачу персональных данных третьей стороне, действующей в качестве агента, организация должна: (I) передавать данные только для конкретных целей; и (II) удостовериться в том, что агент обязуется обеспечить уровень защиты конфиденциальности, как того требуют Принципы; (III) принимать меры, чтобы гарантировать, что агент эффективно обрабатывает персональные данные.; и (IV) требовать от агента уведомлять организации, если он не может выполнять свои обязательства по обеспечению уровня защиты, как требуют Принципы; (V) после направления уведомления, в том числе в рамках (IV), принимать меры для прекращения и устранения несанкционированной обработки; и (VI) предоставить резюме или копию соответствующих положений и договора с агентом Министерству по запросу.

**RECOURSE, ENFORCEMENT AND LIABILITY**

    a. Эффективная защита частной жизни должна включать надежные механизмы обеспечения соблюдения Принципов, обращение за помощью и последствия для организации, когда происходит несоблюдение принципов.  Как минимум такие механизмы должны включать:

     I.) легкодоступные независимые механизмы обжалования, с помощью которых жалобы и споры каждого лица расследуются и оперативно выполняются без каких-либо затрат для данного лица и на основе Принципов, а также возмещения ущерба, если это предусмотрено;

     II.) процедуры действий для проверки достоверности сертификатов, утверждений и практики организаций относительно их практики конфиденциальности и работы при случаях несоблюдения;

    III.) обязательства по устранению проблем, возникающих при несоблюдении Принципов организациями, заявляющими о своей приверженности им, и последствия для таких организаций;

    b. Организации и их отдельные независимые механизмы защиты будут оперативно реагировать на запросы и просьбы Министерства о предоставлении информации, касающейся Privacy Shield. Организации, которые решили сотрудничать с DPAs, включая организации, обрабатывающие данные о людских ресурсах, должны непосредственно реагировать на такие просьбы и жалобы.

    с. Организации обязаны проводить арбитражные разбирательства по искам и соблюдать условия, изложенные в Приложении I, при условии, что какое-либо лицо прибегло к арбитражу, направив уведомление, следуя процедурам в приложении I.

    d. В контексте возможной передачи организация Privacy Shield несет ответственность за обработку личной информации, которую она получает под защитой Privacy Shield и впоследствии передает третьей стороне, действующей от ее имени, если не докажет, что она не несет ответственности за возможный ущерб.

    e. Когда организация становится субъектом FTC или судебного постановления, основанного на несоблюдении, организация предает гласности любые соответствующие разделы, связанные с Privacy Shield. Министерство создало специальный контактный пункт по DPAs по любым проблемам соблюдения организациями Privacy Shield.

**Journalistic Exceptions**

    a. С учетом конституционной защиты свободы печати в США и исключения из директивы журналистских материалов, когда права Свободной Прессы, закрепленные в Первой поправке к Конституции США, пересекаются с интересами защиты частной жизни, Первая поправка должна регулировать баланс этих интересов в отношении деятельности лиц или организаций США.

    b. Личная информация, которая собирается для публикации, трансляции или других форм публичной коммуникации журналистского материала, используется она или нет, а также информация, найденная в ранее опубликованных материалах, распространяемых из медиа-архивов, не подпадает под требования принципов Privacy Shield.

**Secondary Liability**

    a. Интернет-провайдеры ("ISPs"), телекоммуникационные компании и другие организации не несут ответственности в соответствии с принципами Privacy Shield, когда передача, маршрутизация, переключение или кэширование информации происходит от имени другой организации. Как и в случае с самой директивой, Privacy Shield не создает вторичной ответственности.  Так как такая организация действует в качестве простого канала передачи данных как третья сторона и не определяет цели и средства обработки этих персональных данных, она не несет ответственности.

**Performing Due Diligence and Conducting Audits**

а. Деятельность аудиторов и инвестиционных банкиров может включать обработку персональных данных без согласия или знания физического лица. Это допускается принципами, описанными ниже.

b. Публичные фондовые корпорации и компании, находящиеся в тесном контакте, включая организации защиты конфиденциальности, регулярно подвергаются аудиту. Такие проверки могут быть поставлены под угрозу в случае их преждевременного раскрытия, так как проверка может затрагивать информацию о ключевых сотрудниках. Преждевременное раскрытие информации может помешать сделке или даже нарушить действующее регулирование ценных бумаг. Инвестиционные банкиры и адвокаты, осуществляющие должную осмотрительность, или аудиторы могут обрабатывать информацию без ведома физического лица только в той мере и в течение периода, необходимого в обстоятельствах, при которых применение настоящих принципов нанесло бы ущерб законным интересам организации. Эти законные интересы включают в себя мониторинг соблюдения организациями своих юридических обязательств и законной бухгалтерской деятельности, а также необходимость соблюдения конфиденциальности в операциях, осуществляемых инвестиционными банкирами или аудиторами.

**The Role of the Data Protection Authorities**

a. Ниже описан принцип сотрудничества по DPAs.  Под Privacy Shield американские организации, получающие персональные данные из ЕС, обязуются эффективно соблюдать принципы Privacy Shield. Организация должны обеспечить: a) i) обращение за помощью к лицам, к которым относятся данные; (A) (ii) последующие процедуры проверки правильности свидетельств и утверждений, которые они сделали о своей практике конфиденциальности; и(A) (iii) обязательства по устранению проблем, возникающих в результате несоблюдения принципов и последствий для таких организаций.  Организация может выполнять пункты (а) (i) и(А) (iii), если она соблюдает изложенные здесь требования сотрудничества по DPAs.

б. Организация обязуется сотрудничать по DPAs, объявив в своей самосертификации Privacy Shield, что эта организация:

    i. Обязуется удовлетворять требования в пунктах (A)(I) и (A)(III) от Privacy Shield в пунктах Recourse, Enforcement and Liability Principle, соглашаясь сотрудничать по DPAs;

    II. будет сотрудничать по DPAs в ходе расследования и урегулирования жалоб, поданных под Privacy Shield; и

    III. будет выполнять любые рекомендации DPAs, если по DPAs сочтут, что необходимо принять меры для соблюдения Принципов Privacy Shield и представить по DPAs письменное подтверждение того, что меры были приняты.

c. Функции уполномоченного контролирующего органа

    i. Сотрудничество по DPAs будет осуществляться в формате оповещения и консультаций следующим образом:

        1. Рекомендации DPAs будут предоставляться через неофициальную группу DPAs, учрежденную на уровне ЕС, которая поможет обеспечить унифицированный и согласованный подход.

        2. Группа будет консультировать соответствующие организации США по неурегулированным жалобам отдельных лиц на обработку личной информации, которая была передана из ЕС под Privacy Shield.

        3. Группа будет предоставлять такие консультации в ответ на обращения соответствующих организаций и/или жалобы, полученные непосредственно от отдельных лиц в отношении организаций, сотрудничающих по DPAs.

        4. Консультации будут предоставляться только после того, как обе стороны в споре получат разумную возможность высказать свои замечания и представить любые доказательства, которые они пожелают в течение 60 дней после получения.

        5. Группа обнародует результаты рассмотрения жалоб, если сочтет нужным.

        6. Предоставление консультаций через группу не повлечет за собой каких-либо обязательств для группы или для отдельных DPAs.

    ii. Как отмечалось выше, организации, выбирающие этот вариант урегулирования споров, должны взять на себя обязательство выполнять рекомендации DPAs. Если какая-либо организация не выполнит это требование в течение 25 дней с момента консультации и не представит удовлетворительного объяснения задержки, группа уведомляет о своем намерении либо передать этот вопрос федеральному органу или органу штата США, либо заключить, что соглашение о сотрудничестве было серьезно нарушено и поэтому должно считаться недействительным.  В последнем случае группа проинформирует Министерство торговли, с тем, чтобы можно было внести надлежащие изменения в список Privacy Shield.

д. Организация, которая желает, чтобы ее преимущество по Privacy Shield охватывали данные о людских ресурсах, передаваемые из ЕС в контексте трудовых отношений, должна взять на себя обязательство сотрудничать по DPAs в отношении таких данных.

e. Организации, выбирающие этот вариант, должны будут выплачивать ежегодный сбор, который будет рассчитан на покрытие оперативных расходов группы, и им может быть дополнительно предложено покрыть любые необходимые расходы на письменный перевод, возникающие в связи с рассмотрением группой обращений или жалоб на них.  Годовой взнос не будет превышать 500 долларов США и будет меньше для небольших компаний.

**Self-Certification**

a. Преимущества Privacy Shield гарантируются с даты, когда Министерство поместил представление самосертификации организации в список Privacy Shield после определения того, что представление завершено.

b. Для самосертификации Privacy Shield организация должна предоставить министерству представление самосертификации, подписанное корпоративным сотрудником от имени организации, которая присоединяется к Privacy Shield, которое содержит по крайней мере следующую информацию:

    I. название организации, почтовый адрес, адрес электронной почты, номера телефона и факса;

    ii. описание деятельности организации в отношении личной информации, полученной от ЕС; и

    iii. описание политики конфиденциальности организации в отношении такой личной информации, в том числе:

        1. если организация имеет открытый веб-сайт, соответствующий веб-адрес, где доступна Privacy Policy, или если организация не имеет открытого веб-сайта то, где Privacy Policy доступна для просмотра общественностью;

        2. дата его вступления в силу;

        3. контактное бюро для обработки жалоб, запросов на доступ и любых других вопросов, возникающих в рамках Privacy Shield;

        4. конкретный подзаконный орган, который обладает юрисдикцией для рассмотрения любых претензий к организации;

        5. название любой программы конфиденциальности, членом которой является организация;

        6. метод проверки (например, внутренняя, третья сторона) (см. дополнительный принцип проверки; и

        7. независимый механизм обжалования, который доступен для расследования неурегулированных жалоб.

c. Если организация желает, чтобы ее преимущества по Privacy Shield охватывали информацию о людских ресурсах, передаваемую из ЕС для использования в трудовых отношениях, она может сделать это в тех случаях, когда подзаконный орган, указанный в Принципах, обладает юрисдикцией для рассмотрения претензий к организации, возникающих в связи с обработкой информации о людских ресурсах, а также необходимо указать это в самосертификации, заявить о сотрудничестве с соответствующем органом и выполнении рекомендации от этого органа. Организация необходимо предоставить министерству копию Privacy Policy и предоставить просмотр ее затронутыми сотрудниками.

д. Министерство ведет список организаций, которые подают заполненные документы о самосертификации. Заявления о самосертификации должны представляться не реже одного раза в год; в противном случае организация будет исключена из списка защиты конфиденциальности, и преимущества Privacy Shield больше не будут гарантироваться. Организации в списке Privacy Shield публично заявляют, что придерживаются Принципов. Privacy Policy организации, если она доступна в режиме онлайн, должна включать гиперссылку на веб-сайт Privacy Shield Министерства и гиперссылку на веб-сайт или форму подачи жалобы независимого механизма обжалования, который доступен для расследования неурегулированных жалоб.

e. Принципы конфиденциальности применяются сразу же после самосертификации. Признавая, что Принципы будут влиять на коммерческие отношения с третьими сторонами, организации, удостоверяющие Privacy Shield Framework в течение первых двух месяцев со вступления PSF в силу, максимально быстро (не позднее девяти месяцев с даты удостоверения) приведут существующие коммерческие отношения с третьими сторонами в соответствие с Принципом ответственности за последующую передачу.

f. Организация должна относить к принципам Privacy Shield все персональные данные, полученные от ЕС в зависимости от Privacy Shield.  Соблюдение обязательств не ограничено по времени присутствия в Privacy Shield, даже если впоследствии она по какой-либо причине покидает Privacy Shield, но в случае, когда организация, которая выходит из Privacy Shield хочет сохранить данные, она должна подтвердить Министерству на ежегодной основе соблюдение Принципов и адекватной защиты информации. В противном случае организация должна вернуть или удалить информацию.  Организация, которая выходит из Privacy Shield, должна удалить из политики конфиденциальности любые ссылки на Privacy Shield, подразумевающие участие организации в Privacy Shield.

g. Организация, которая прекратит свое существование в качестве отдельного юридического лица в результате слияния или поглощения, должна заранее уведомить об этом Министерство.  В уведомлении следует указать, будет ли приобретающая организация, возникшая в результате слияния, i) по-прежнему связана Принципами Privacy Shield действием закона, регулирующего поглощение или слияние, или ii) решит самостоятельно подтвердить свою соблюдение Принципов Privacy Shield или ввести другие гарантии, такие как письменное соглашение.  Если ни (i), ни (ii) не применяются, любые персональные данные, которые были приобретены под Privacy Shield, должны быть незамедлительно удалены.

h. Когда организация покидает Privacy Shield по какой-либо причине, она должна удалить все заявления об участии в Privacy Shield, удалить сертификационный знак EU-U. S. Privacy Shield, если он используется. Искажения информации могут быть обжалованы FTC или другим соответствующим государственным органом, или в соответствии с Законом о ложных заявлениях (18 U. S. C. § 1001) могут быть поданы иски в адрес Министерства.